FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™ MAJOR UPDATE

GNFA Network Forensic Analyst | CyberLive
giac.org/gnfa

6 Day Program	36 CPEs	18 Labs

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL/TLS traffic to identify attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage meddler-in-the-middle tools to intercept seemingly secure communications

Who Should Attend

- Incident response team members
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Security Operations Center (SOC) personnel and information security practitioners
- Network defenders
- Information security managers
- Network engineers
- Information technology professionals

NICE Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Philip Hagen
Course Author

Take your system-based forensic knowledge onto the network. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. SANS FOR572™ covers the tools, technology, and processes required to integrate network evidence sources into your investigations to provide better findings, and to get the job done faster.

In FOR572,™ we focus on the knowledge necessary to examine and characterize communications that have occurred in the past or continue to occur. Even if the most skilled remote attacker has compromised a system with an undetectable exploit, the system must still communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: bad actors are talking—we'll teach you to listen.

Business Takeaways

- Round out your team's investigations to include network perspectives inherent in all environments
- Build baselines that can be used to proactively identify malicious activity early in a compromise, before large-scale damage is done
- Provide additional value for existing network data collections that support existing operational requirements
- Ensure critical observations from the network are not overlooked in proactive hunting or post-compromise IR actions

Syllabus Summary

SECTION 1: Off the Disk and Onto the Wire

SECTION 2: Core Protocols and Log Aggregation/Analysis

SECTION 3: NetFlow and File Access Protocols

SECTION 4: Commercial Tools, Wireless, and Full-Packet Hunting

SECTION 5: Encryption, Protocol Reversing, OPSEC, and Intel

SECTION 6: Network Forensics Capstone Challenge

"Phil is probably one of the best instructors I've ever learned from. He's an excellent guy, smart, has a ton of relevant industry knowledge that he can bring in while teaching, and knows how to keep the content interesting."

—Ronald B.

For detailed course description, visit **SANS.ORG/FOR572**

WAYS TO TAKE FOR572

In-Person | **Live Online** | **OnDemand**